

Installation & configuration user guide of Ping Federate



ASR 2006/2007 Final Project

Supervisors: Maryline Maknavicius-Laurent, Guy Bernard

SOMMAIRE

<u>I.</u>	<u>LDAP SERVER INSTALLATION AND CONFIGURATION</u>	<u>2</u>
A.	SERVER INSTALLATION	2
B.	SERVER CONFIGURATION	3
C.	RUNNING THE SERVER	4
D.	CREATING ENTRIES	4
E.	LDAP CLIENT	5
F.	SOME LINKS	6
<u>II.</u>	<u>POSTFIX MAILSERVER INSTALLATION</u>	<u>7</u>
A.	INSTALLATION	7
B.	CONFIGURATION	7
C.	IMAP SERVER	7
D.	LAUNCHING	8
E.	SENDING E-MAIL WITH TERMINAL MODE	8
F.	MAIL CLIENT	8
G.	SOME LINKS	9
<u>III.</u>	<u>J2SE INSTALLATION</u>	<u>10</u>
<u>IV.</u>	<u>TOMCAT SERVER INSTALLATION</u>	<u>10</u>
A.	STANDARD INSTALLATION	10
B.	RUNNING THE SERVER	11
C.	ADMINISTRATION TOOLKIT INSTALLATION	12
D.	SETTING-UP THE USERS' AUTHENTICATION	12
1.	DEFAULT CONFIGURATION	12
2.	LDAP-USING CONFIGURATION	14
E.	USEFUL LINKS	17
<u>V.</u>	<u>INSTALLING AND CONFIGURING PING FEDERATE</u>	<u>17</u>
A.	CONFIGURATION	17
<u>VI.</u>	<u>THE SCENARIOS WE HAVE TESTED</u>	<u>21</u>
A.	FIRST CASE: LOCAL TEST	21
B.	SECOND CASE: TEST WITH ITAM	22
C.	THIRD CASE: TEST WITH LDAP	26
	<u>APPENDIXES</u>	<u>28</u>

We had two computers to work with. The first we have been given, '**cubitus**' **computer**, had 6GiB memory available with fixed IP address **157.159.103.165**. The second computer provided, '**ventenpoue**' **computer**, had 31,50 GiB memory available, with fixed IP address **157.159.100.76**. We installed **Ubuntu** O.S on each computer. The LDAP server, Postfix mail server, and Ping Federate server, were installed on cubitus computer (because it was the only computer we had at this time). The Tomcat server was installed on ventenpoue computer.

I. LDAP SERVER INSTALLATION AND CONFIGURATION

Ping Federate aims to federate identities, which suggests databases or directories (such as LDAP). Indeed, before adding a Ping Federate server, some services already exist with associated authentication via databases or directories. Initial user authentication can use an application or IdM (Identity Management) system logon module (for a set of internal services proposed within a same enterprise for example).

Including Ping Federate servers enables a user having previously access to a circle of trust (set of services in a same domain, for example .int-evry.fr) to be able to access services from another circle of trust, without having to pass through local authentication. This is possible because Ping Federate servers can interact with existing databases or directories.

We have chosen to use a LDAP directory because PingFederate packages an LDAP Authentication Service Adapter and logon form that can authenticate users directly against an LDAP data store. It was interesting because we did not have already a centralized local authentication service. Thanks to this LDAP adapter, it will be possible to authenticate to our IdP via a pop-up authentication window (searching in our LDAP database).

A. Server installation

LDAP, Lightweight Directory Access Protocol, is an Internet protocol that email and other programs use to look up information from a server. LDAP is appropriate for any kind of directory-like information, where fast lookups and less-frequent updates are the norm.

To install LDAP server, we downloaded the following packages via Synaptic Package Manager (reachable via [System>Administration>Synaptic Package Manager](#)):

- ldap-utils
- libldap-2.2-7
- libldap2-dev
- slapd

The password for the LDAP server is '**liberty**'.

B. Server configuration

The configuration file can be found at */etc/ldap/slapd.conf*. A copy of this file is in the appendix. Here are some comments about this file:

- The following line enables the use of v2 standard of LDAP:
allow bind_v2
- The following line indicates the root of LDAP database:
"dc=mondomaine,dc=com"

The database administrator is under the distinguished name '**cn=admin,o=INT,c=FR**'. The password is '**liberty**'. To enable this, the following line must be added manually:
rootdn "cn=admin, dc=mondomaine, dc=com"

The following line, that must be added manually, gives the password:
rootpw admin

For better security, it is advised to generate an encrypted password using the following command:

```
> slappasswd  
>New password:  
>Re-enter new password:  
{SSHA}rdh5747747LDHDFHMDFHDDHD
```

Then, the encrypted password must be copied instead of the former unencrypted password. To enable write rights on the base, the root of the base and the right login must be indicated:

```
access to attribute=userPassword  
by dn="cn=admin,dc=mondomaine,dc=com" write  
by anonymous auth  
by self write  
by * none
```

To enable the read-only access of the base, the root of the base and the right login must be also indicated:

```
access to *  
by dn="cn=admin,dc=mondomaine,dc=com" write  
by * read
```

C. Running the server

The LDAP server can be launched by the following command:

```
> slapd -d 5 -h ldap://localhost:9009/ -f /etc/ldap/slapd.conf
```

The “d” parameter tells the server to display events. The “good” values are 4 or 5, depending on the number of messages displayed.

The “h” parameter specifies the port number of the server.

The “f” parameter specifies the configuration file to be read by the server.

(from <http://www-public.int-evry.fr/~gardie/LDAP/TP/TP1-cadre.html>)

D. Creating entries

Entries are generally sent to the server from text files describing the attributes (and their values) for each entry. The format of these text files is standardized: it uses the LDIF syntax.

The database file (.ldif and utf8) are saved under **/home/liberty/base_ldap/**.

These are the ldif files that we used to fill the LDAP directory:

```
dn: cn=Eunice, o=INT, c=FR
objectclass: inetOrgPerson
cn: Eunice
sn: Mondesir
mail: eunice.mondesir@int-evry.fr
userPassword: stella

dn: cn=Pierre, o=INT, c=FR
objectclass: inetOrgPerson
cn: Pierre
sn: Weill-Tessier
mail: pierre.weill_tessier@int-evry.fr
userPassword: antoine
```

Figure 1: file int_1.ldif

```
dn: cn=Maryline, o=INT, c=FR
objectclass: inetOrgPerson
cn: Maryline
sn: MAKNAVICIUS
mail: Maryline.MAKNAVICIUS@int-evry.fr
userPassword: mdpMaryline
title: user

dn: cn=Francisco, o=INT, c=FR
objectclass: inetOrgPerson
cn: Francisco
sn: MENDEZ
mail: truc.machin@int-evry.fr
```

```
userPassword: mdpFrancisco
title: bidon

dn: cn=Uciel, o=INT, c=FR
objectclass: inetOrgPerson
cn: Uciel
sn: FRAGOSO
mail: truc.machin@int-evry.fr
userPassword: mdpUciel
title: admin
```

Figure 2: file ajout.ldif

The ‘title’ attribute will be used for the authentication to access our test service (INTest) under Tomcat (cf. Tomcat server installation part).

To convert an LDIF file into an UTF8 file, the following command must be typed:

```
> iconv -f ISO_8859-1 -t UTF-8 -o file.utf8 file.ldif
```

It is useful if the LDIF contains special characters such as “é” or “ß” or “p”.

To add entries, the following command must be done:

```
> ldapadd -w secret -D "cn=Manager,o=INT,c=FR" -x -H ldap://hostname:9009/ -f file.utf8
```

In which :

- The “w” parameter gives the required password to be authenticated by the server (rootpw).
- The “D” parameter indicates the manager name of the database (rootdn).
- The “x” parameter tells that the authentication method is simple.
- The “H” parameter indicates the host name (ldap://host:port) and the port needed to access to the server.
- And finally, the “f” parameter gives the file name of an LDIF/UTF8 file.

E. LDAP Client

To manage the LDAP base it is possible to install LDAP clients allowing easy modifications of the base. We installed **ldapbrowser** client because its installation and use were quite simple. For a future use, we advise to use an LDAP client who already integrates the inetOrgPerson class or to seek if it is possible to add this class in ldapbrowser.

The entries added in our LDAP directory can be seen on this ldapbrowser screenshot:

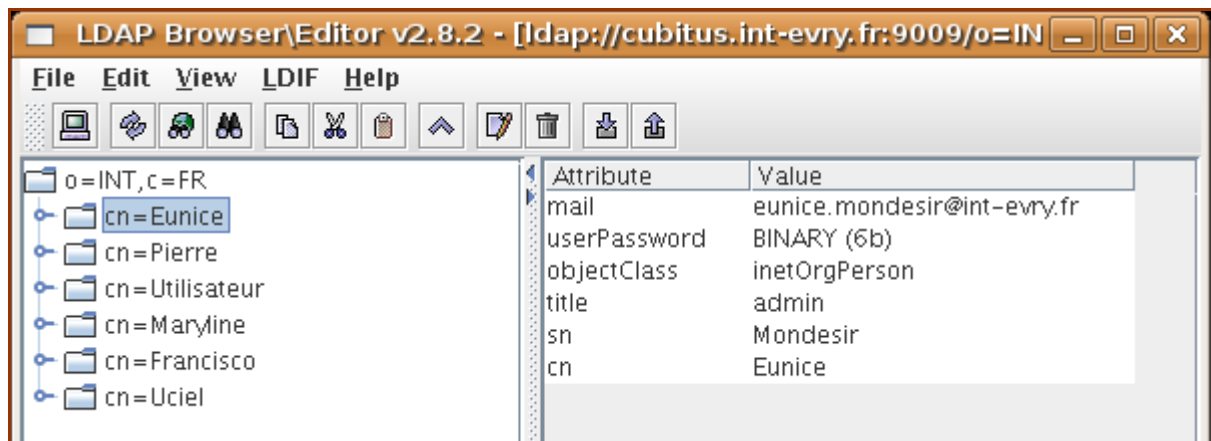


Figure 3: ldapBrowser screenshot

F. Some links

Here are some useful links to go further (the links are in french):

<http://blog.thelinuxfr.org/index.php/post/2006/09/01/56-installation-et-configuration-d-un-serveur-lda>

Installation and configuration of a LDAP server with (K)Ubuntu

<http://www-public.int-evry.fr/~gardie/LDAP/ListeTP.html>

LDAP labs of Mr Michel GARDIE, professor at INT

Links about CAS (Central Authentication Service):

http://fr.wikipedia.org/wiki/Central_Authentication_Service

<http://www.ja-sig.org/products/cas/index.html>

http://www.esup-portail.org/consortium/espace/SSO_1B/cas/jres/cas-jres2003-article-web.htm#_Toc52002547

II. POSTFIX MAILSERVER INSTALLATION

A. Installation

We have installed a mail server on cubitus computer for Ping Federate server to send notifications (i.e. when the licence happens to be out-of-date). The mail server we used is Postfix. We installed it by downloading the following packages in Synaptic Packages Manager:

- postfix
- postfix-dev
- postfix-doc
- Mailx

B. Configuration

Postfix configuration file can be found in **/etc/postfix/main.cf**. A copy of this file is in the appendix. In this file:

- myhostname : is the name of the mailserver
- home_mailbox = Maildir/ : this line must be added to the configuration file in order to receive the mails by IMAP!

C. IMAP server

We have also installed an IMAP server as a MDA (Mail Delivery Agent). To do so, we had two equivalent possibilities:

- installing courier-imap package in Synaptic Packages Manager
- making the following command:

```
> sudo apt-get install postfix courier-imap
```

We didn't choose to install a LDAP (or other database) Postfix package because there is only one administrator for the mail server/PF server. Therefore, only one email account is needed. The username/password of this account are those of the Linux user account for this computer (**liberty,liberty**).

'Courier-imap' configuration file can be found in **/etc/courier/imapd**.

In this configuration file, the last line must be changed as following:

MAILPATH = Maildir

Once this MAILPATH positioned, the following command must be done in the HOME directory :

```
> maildirmake Maildir
```

This will create the mailbox **Maildir/** in the HOME directory.

D. Launching

The following command enables to launch postfix and courier-imap:

```
> sudo /etc/init.d/postfix restart && sudo /etc/init.d/courier-imap restart  
&& sudo /etc/init.d/courier-authdaemon restart
```

E. Sending e-mail with terminal mode

In order to send mails thanks to the 'mail' Linux command (console mode), we have installed Mailx. The command is 'mail + recipient' as showed in the following example :

```
> mail eunice.mondesir@int-evry.fr  
Subject: Test  
Identity Federation is very cool  
Cc:  
>
```

Between each field, you must tape the [Enter] key. After the 'Cc' field, you must tape [Enter] key, then [CTRL]+[D].

Both MTA(Mail Transfer Agent) and MDA(Mail Delivery Agent) have been installed on cubitus: we don't expect to receive/send many emails, since this mailbox is only dedicated to send automatic notifications.

F. Mail Client

In order to check the received mails, we have installed the MUA (Mail User Agent, mail client) Mozilla Thunderbird. To do that, we installed "mozilla-thunderbird" package.

The requested parameters for the configuration of Thunderbird are (they can be modified in [Edit>account parameters](#) for the Linux thunderbird):

- Account Name (optional) : Liberty
- Email Address : liberty@cubitus.int-evry.fr
- Password : liberty (Linux user password)

Servers parameters :

- IMAP server (MDA) : 157.159.103.165 port 143 (cubitus IP)
- SMTP server (MTA) : 157.159.103.165, port 25

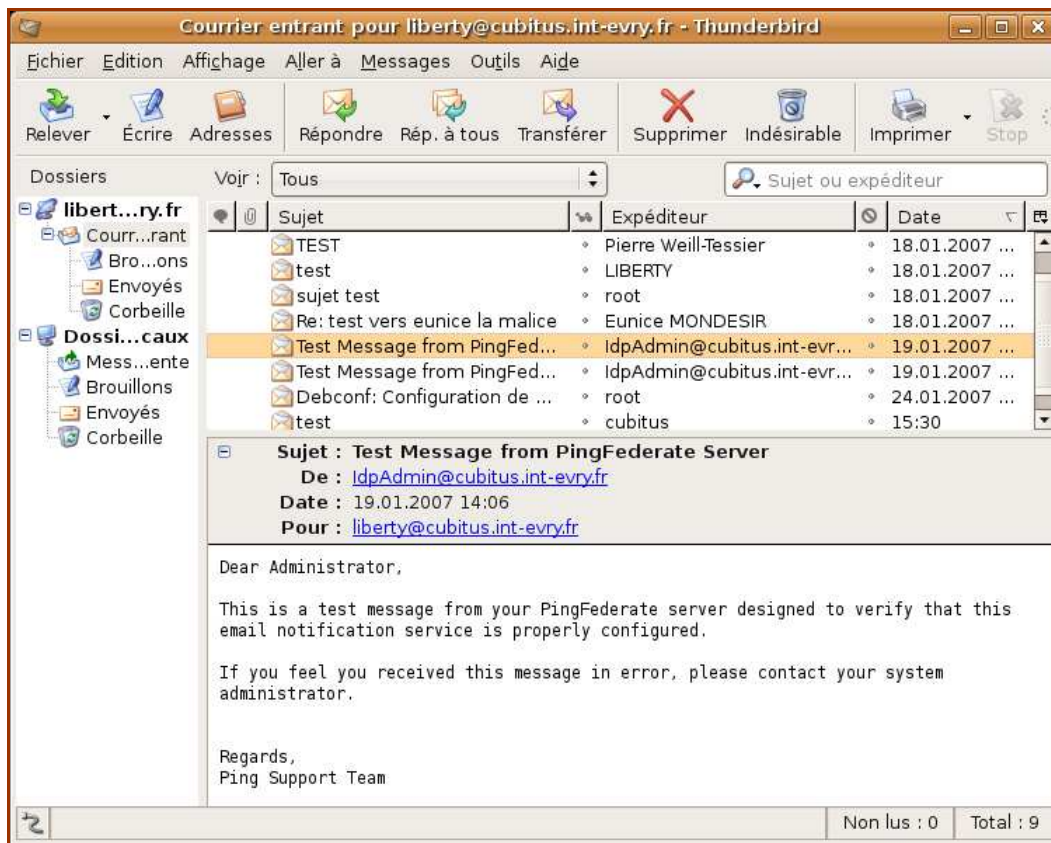


Figure 4: Thunderbird MailClient

We have tried different use cases to test the sending/receiving functions of our servers. We can send to every email addresses; but we can only receive from INT email addresses. Nevertheless, this is not very important, since we suppose the administrator being an INT staff, and the servers are in a subnetwork of INT (the notifications mails will only be sent to INT addresses).

G. Some links

Installation and configuration of postfix:

http://www.coagul.org/article.php3?id_article=192

<http://www.linux-france.org/article/mail/postfix-jaco/#N3121>

<http://doc.ubuntu-fr.org/serveur/mail>

Postfix documentation(english and french):

<http://www.postfix.org/documentation.html>

<http://x.guimard.free.fr/postfix/>

III. J2SE INSTALLATION

Ping Federate and Tomcat both require J2SE to run. The installation of J2SE is rather easy: please download the version of J2SE you need on <http://java.sun.com/javase/downloads/index.jsp>

The latest version of Ping Federate we have installed uses J2SE 1.5. This is the version installed on the 'cubitus' computer.

Tomcat may use J2SE 1.4 and J2SE 1.5, but to be homogenous with the choice we had made on 'cubitus' computer, we have installed J2SE 1.5.

Please refer to the installation guide provided on Sun's web site when downloading J2SE for more information about setting up the Java environment.

For your information about the variables JAVA_HOME and PATH we used in both computers' `.bashrc` files.

IV. TOMCAT SERVER INSTALLATION

As we didn't have any web service that ran inside our circle of trust, we have decided to use Tomcat as a web application server. The reason is firstly because the application samples provided by Ping Federate run under Tomcat, and also because it is a strong tool that supports both standard web language (html), and java application by the means of servlets.

As we have explained before, Tomcat server has been installed on the 'ventenpoupe' computer.

We are going to describe now the procedure of a standard installation of Tomcat, followed by some modifications in order to use the LDAP database we have set before.

A. Standard installation

The installation package is available at <http://tomcat.apache.org>, under the menu 'downloads'. The version of Tomcat to download depends of the J2SE configuration. In any case, you **must have J2SE installed** on the 'ventenpoupe' computer before going ahead.

Since the version of J2SE we require is 1.5, the right version of Tomcat to download is Tomcat 5. We have installed Tomcat 5.5.20.

Once you have reached the 'downloads' menu, you can click on the [5.5.20](#) link and start downloading the core distribution. You will also need to download the 'Administration Web Application' if you want to use the administration toolkit (refer to the section dealing with the topic for more information).

Create or choose a folder to extract the server files. (We have chosen the path `~/apache-tomcat-5.5.20`.)

You finally need to set the environment variable `CATALINA_HOME` to the path of your server (e.g. `CATALINA_HOME = ~/apache-tomcat-5.5.20`), and add to the variable `PATH` the folder **`CATALINA_HOME/bin`** and all the jar libraries to the `CLASSPATH` variable. To check how to set up these variables, 'ventenpoupe's **`.bashrc`** file has been added to the appendices.

B. Running the server

The Tomcat server can be launched or stopped by the following commands:

- > `$CATALINA_HOME/bin/startup.sh` (to launch)
- > `$CATALINA_HOME/bin/shutdown.sh` (to stop)

The main page of Tomcat is reachable once you have started the server, by the URL `http://<tomcat_server_address>:<tomcat_port>` (e.g. <http://ventenpoupe.int-evry.fr:8080/>).

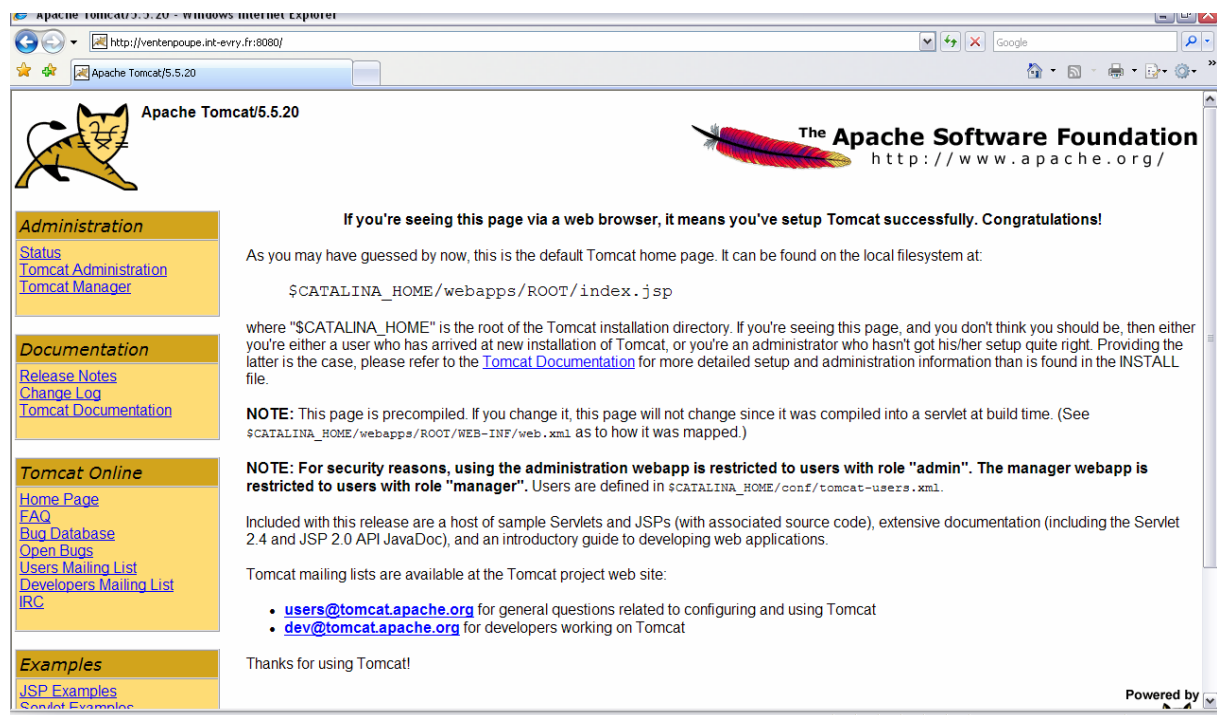


Figure 5: main page of the Tomcat server

C. Administration toolkit installation

The core distribution of Tomcat server does not include the administration toolkit for security reason. If needed, the toolkit can easily be installed.

Under the same web page presented before, download the 'Administration Web application' if you have never done it. Extract the downloaded file and copy the folders in the Tomcat server's directory structure as follow:

- Go to **server/webapps/** and copy the folder **admin** into **CATALINA_HOME/server/webapps/**,
- Go to **config/Catalina/localhost** and copy the file **admin.xml** into **CATALINA_HOME/config/Catalina/localhost/**

Here is the service you should be able to access from your browser at the address `http://<tomcat_server_address>:<tomcat_port>/admin`.

(e.g. <http://ventenpoupe.int-evry.fr:8080/admin>)

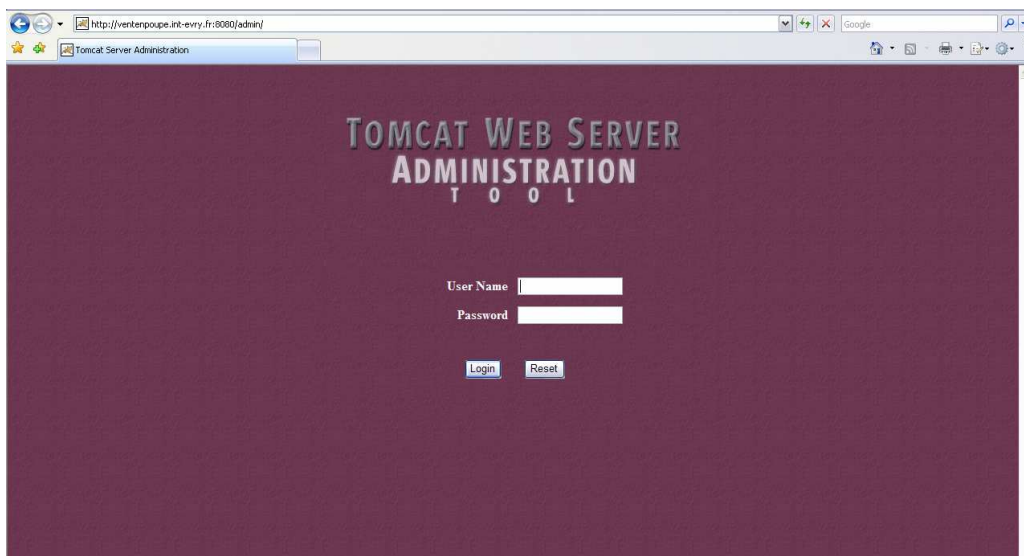


Figure 6: Tomcat administration tool page

As you can see from the above figure, Tomcat uses an authentication system that is needed to set up at the first use. The following part explains how to do so.

D. Setting-up the users' authentication

Tomcat proposes different way of configuring the users' authentication for the hosted applications. Regarding our case, only two of them are relevant: the default one, which is a stand-alone authentication, and one using a LDAP database. Both configurations are being explained.

1. Default configuration

Tomcat initially provides a configuration file for setting this authentication list. This file is called **tomcat-users.xml**, situated in the path **\$CATALINA_HOME/config**.

As the following example of this file, you can set the users' authentication policy as you wish:

```
<tomcat-users>
  <role rolename="user"/>
  <role rolename="manager"/>
  <role rolename="admin"/>
  <user username="alliance" password="liberty" roles="manager,admin"/>
</tomcat-users>
```

Figure 7: example of the tomcat-users.xml file

The 'role' tag allows you to create roles. Note that for the administration service and the management service included in Tomcat you must set up the 'admin' and 'manager' roles.

The 'user' tag allows you to associate and define the authentication's attributes of all the users. The 'username' attribute sets logins, the 'password' attribute sets the password of the user associated to the username, and the 'roles' attributes set the role(s) associated to this username.

You may want to set the authentication process to several applications. Tomcat allows you to indicate the application whether any authentication is required, in the file **web.xml** of the **WEB-INF/** directory of your application's folder (which is usually under **\$CATALINA_HOME/webapps/**). An example gives you an idea of how setting this file for an application.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<web-app>
  <display-name>INTest</display-name>
  <resource-env-ref>
    <resource-env-ref-name>users</resource-env-ref-name>
    <resource-env-ref-type>org.apache.catalina.UserDatabase</resource-env-ref-type>
  </resource-env-ref>

  <security-constraint>
    <web-resource-collection>
      <web-resource-name>Secure Page</web-resource-name>
      <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <description>These roles are allowed access</description>
      <role-name>user</role-name>
    </auth-constraint>
  </security-constraint>

  <login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>INT</realm-name>
  </login-config>

  <security-role>
    <description>role is required to log in to the INTest Application</description>
    <role-name>user</role-name>
  </security-role>
</web-app>
```

Figure 8: example of 'web.xml' for the INTest application

- In the 'authen-method' tag, **BASIC** refers to a login popup from the browser (cf. following figure). This is the easiest way of configuring the identification.
- The 'role-name' tag, you must indicate the user's role that is allowed to use the application.
- The 'url-pattern' tag allows configuring the scope of the security constraint. The path you specify is a relative path from the 'context' path of Tomcat. (See the Tomcat Doc for more detail). You can add as many tags as you wish, according to the scope you choose.

You can check for more details on the Internet (cf. Useful Information)

2. LDAP-using configuration

After being sure your LDAP database has been properly installed (cf. LDAP Server Installation and Configuration part), you can use LDAP as a database for Tomcat to realise authentication, instead of the default authentication that Tomcat includes.

To do so, you need to install an API for Tomcat to communicate with LDAP, indicated Tomcat how to find your database, and homogenate the attributes used by LDAP and Tomcat.

- installation of the APIs

The API between Java language and LDAP is part of Sun's JNDI interface that you can download from the following web site:

<http://java.sun.com/products/jndi/downloads/index.html>.

We have downloaded JNDI 1.2.1 which includes all the LDAP APIs required for using LDAP in a Java-language environment.

Choose the place you want to extract what has been downloading. You should have three folders corresponding to the parts of the download: JNDI, LDAP and LDAPBP.

Each part contains a **lib/** directory of jar libraries. To make Tomcat using these libraries, it is required to move the content of the three **lib/** directory in to Tomcat's libraries directory: **\$CATALINA_HOME/server/lib/**.

The final step to install the APIs is adding the libraries to the variable CLASSPATH of the **.bashrc** file. (see the example in the appendix)

If you need to get into the JNDI classes, the official Java Doc is here: <http://java.sun.com/jndi/1.2/javadoc/index.html>.

- indicate tomcat how to find the terminal

Configuration of Tomcat to reach the LDAP database is made in the file **server.xml**, in the directory **\$CATALINA_HOME/config/**.

Here are indications to set it up accordingly with our environment:

In the ‘Server/Service/Engine’ add the following tag

```
<Realm className="org.apache.catalina.realm.JNDIRealm" debug="99"  
    connectionURL = "ldap://cubitus.int-evry.fr"  
    userBase = "o=INT,c=FR"  
    userSearch = "(cn={0})"  
    userRoleName = "title"  
</>
```

Figure 9: 'realm' tag in 'server.xml' in Tomcat

The ‘className’ attribute specify which adapter Tomcat must use (as we said there are many ways to configure authentication, but the value indicated here **is the only one to use** when working with JNDI and LDAP).

The ‘connectionURL’ attribute specify the database address.

The ‘userBase’ is the root DN of the LDAP database.

The userSearch is the filter on the database to identify the user from the login entered in the popup, against the LDAP database. The token {0} is related to the login entered.

The userRoleName is the attribute in LDAP which corresponds to the role that Tomcat checks for authorizing authentication on an application. Here, we chose the attribute ‘title’ which is available for the LDAP class ‘inetOrgPerson’. The attribute ‘title’ can takes the following values ‘admin’ (to access administrator service), ‘manager’ (to access the management service) and ‘user’ (to access INTest test service, our application).

Here is the authentication form on the service we have made (INTest) and the main page of the service:

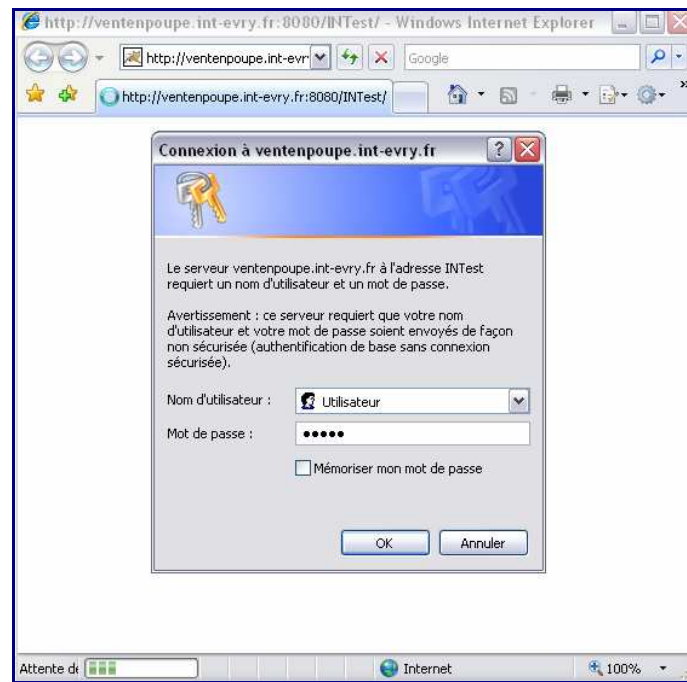


Figure 10: authentication popup on the Tomcat INTest service

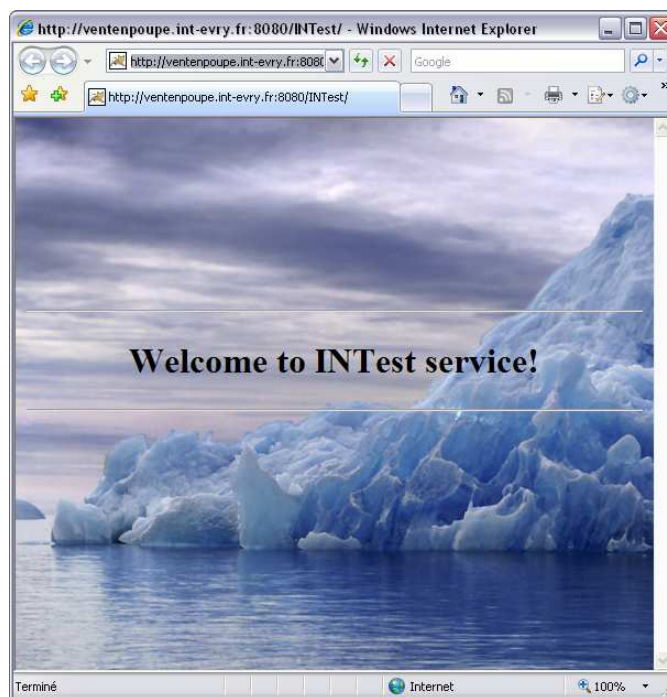


Figure 11: Tomcat INTest service main page (after authentication)

E. Useful links

To install the security policy on Tomcat:

<http://www.agora.2ia.net/mediawiki/index.php?title=Tomcat>

<http://tomcat.apache.org/tomcat-5.5-doc/jndi-resources-howto.html>

<http://beuss.developpez.com/tutoriels/tomcat/authentication/formulaire/>

For general information:

<http://www-igm.univ-mlv.fr/~dr/XPOSE2003/tomcat/tomcat.php?rub=20>

<http://www-inf.int-evry.fr/cours/WebServices> (Samir TATA's teaching labs page,INT)

V. INSTALLING AND CONFIGURING PING FEDERATE

To install Ping Federate, you must download the product archive at the following website: <http://pingfederate.com/products/pingfederate/download>. Since we were not concerned about the background of the structure we had to deploy Ping Federate, we have chosen to install the latest version, Ping Federate 4.2.

Note that you will require a license to use Ping Federate for free during 90 days or the first 100.000 transactions, whichever comes first. It needs 2 working days max to receive the license, so be aware of the fact that during this gap, you CAN NOT set up Ping Federate.

As we have seen, Ping Federate server can play the role of an IdP or an SP, or both. According your infrastructure and policy, you may need to install Ping Federate on different computers, with dedicated roles.

In our case, one computer is used to play the role of an IdP and a SP (the 'cubitus' computer).

The installation itself is not difficult; we invite you to consult the **PingFederate_Admin_Manual.pdf** file to follow the installation instructions, located in the directory **docs/** of Ping Federate folder.

The main page of the server (https://<pingferate_server_name>:<pingfederat_port>/pingfederate/app, for example <https://cubitus.int-evry.fr:9999/pingfederate/app>) loads a web application that allows you to configure the server, according the settings you want.

In our case, the login and password for administrating the Ping Federate server are:

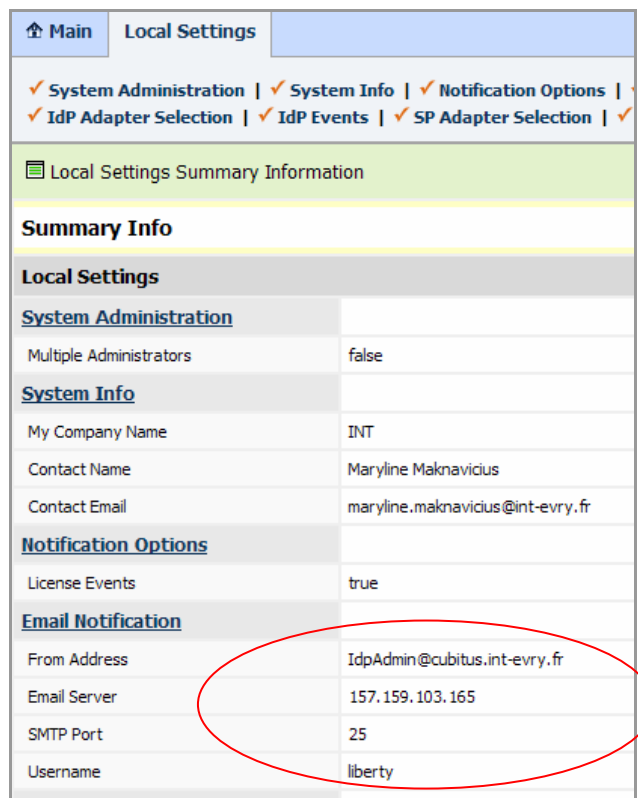
- administrator
- PWTa24ae2!

A. Configuration

Once again, **PingFederate_Admin_Manual.pdf** is documented enough for you to configure the server. Nevertheless, the next figures and explanations will provide you some information you may require, according to our configuration.

- Local settings:

The figure below shows the settings you must enter if you choose to activate email notification. You must specify the address and the port from the server you want to use for sending a notification email, under the account you specify in the 'From Address' field, to a account. **Both email addresses must contain the same domain part.** The user part of the 'From Address' can be not related to an existing account.



Local Settings	
System Administration System Info Notification Options IdP Adapter Selection IdP Events SP Adapter Selection	
Local Settings Summary Information	
Summary Info	
Local Settings	
<u>System Administration</u>	
Multiple Administrators	false
<u>System Info</u>	
My Company Name	INT
Contact Name	Maryline Maknavicius
Contact Email	maryline.maknavicius@int-evry.fr
<u>Notification Options</u>	
License Events	true
<u>Email Notification</u>	
From Address	IdpAdmin@cubitus.int-evry.fr
Email Server	157.159.103.165
SMTP Port	25
Username	liberty

Figure 12: local settings page of Ping Federate server

- IdP adapters

We have installed two adapters: a standard adapter, and a LDAP adapter.

For the standard adapter, the configuration has been set according to the manual; the only part to care about is that we put the 'Logout Service' and 'Authentication Service' fields contain the address 'http://ventenpoupe.int-evry.fr:8080' which refers to our Tomcat server.

In the following summary of the LDAP adapter, we can see the filter's settings to perform the database's entries (cn={username}, where {username} is a token that corresponds to the login entered in the authentication form that provides the adapter).

Main	Manage IdP Adapter Instances	Create Adapter Instance
✓ Adapter Type ✓ IdP Adapter ✓ Adapter Attributes ✖ Summary		
IdP adapter instance summary information.		
Summary Info		
Create Adapter Instance		
<u>Adapter Type</u>		
Adapter Instance Name	LDAPINT	
Adapter Instance Id	LDAPINT	
Adapter Type	PF4 LDAP Authentication Service v1.0	
Adapter Class Name	com.pingidentity.adapters.ldap.idp.LdapIdpAuthnAdapter	
<u>IdP Adapter</u>		
LDAP Datastore	LDAP-2343F3AE0AB20E651B4C718D53D5FB24ECE3A92A	
Search Base	o=INT,c=FR	
Search Filter	cn=\${username}	
Realm	INTest	
Scope of Search	SUBTREE_SCOPE	
Connection Pooling	false	
Operational Mode	BASIC_AUTHN	
Challenge Retries	3	
<u>Adapter Attributes</u>		
userId	selected	

Figure 13: LDAP adapter summary

Note that before installing this adapter you need to set the database connection.

- Data Store

Main	Manage Data Stores	Data Store
✖ LDAP Configuration ✓ Summary		
Please provide the details for configuring this LDAP connection.		
Hostname	cubitus.int-evry.fr:9009	*
☐ Bind Anonymously		
Username	cn=admin,o=INT,c=FR	*
Password	••••••	
☐ Use SSL		
☐ Mask Values in Log		

Figure 14: Data Store configuration summary

This menu allows connecting the database to the Ping Federate server, with the parameters of the LDAP database's administrator (cf. [LDAP part](#)).

- SAML Metadata Export

The metadata file (xml) can be automatically created under this menu. You have the choice to edit the role from which the metadata is from, and then send it to your partners.

- Configuring the partner's connections

This part of Ping Federate mainly depends on the scenarios that you plan to deploy with your partners. Refer to the manual for understanding the general overview, and the notice for a more detailed presentation with our case study.

Note that the IdP's parameters of your partners are set in your IdP connections page, *where appear the SP adapter(s) you want them to use*; and the SP's parameters of your partners are set in your SP connections page, *where appear the IdP adapter(s) you want them to use*.

Logically, your partners should have done the same the other way wrong. Once this is done, the connections are set up to allow communications between the Ping Federate servers.

The figure shows an example of a configuration (cf. the scenarios part of the manual for more details).

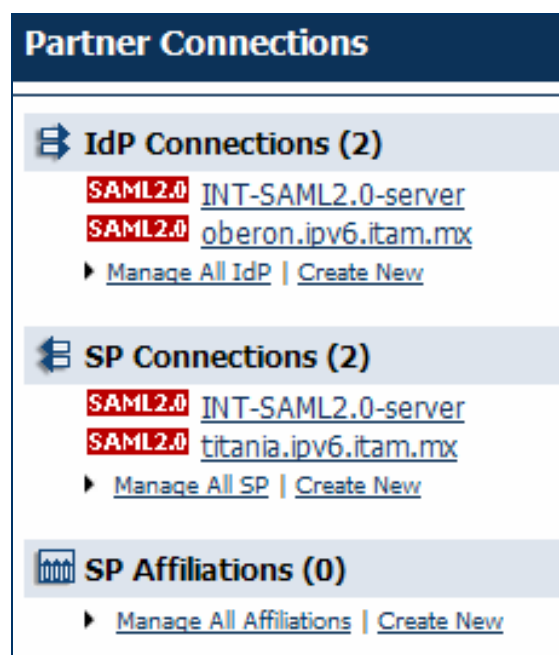


Figure 15: example of the partners connection in Ping Federate server admin page

VI. THE SCENARIOS WE HAVE TESTED

In the project case, we have tried 3 scenarios we are going to explain here. The first one is a local test, the second one is a test with ITAM in Mexico, and the third one is our application test.



During the tests, we have noticed that browsers (Mozilla Firefox and Microsoft Internet Explorer) keep login-information. Therefore, you may activate SLO or local sign-out, but the browser will still remember your identity.

You must close the browser window to erase your identity parameters!

A. First case: local test

This case is the example provided by the [Quick_Star_Guide.pdf](#) file (located in the [quickstart/docs](#) repertory of Ping Federate).

With the applications samples provided by Ping Federate, we will simulate an IdM and service applications, which are running under Tomcat server and that will both be in our circle of trust. That is to say, the 'ventenpoupe' computer will host both IdP and SP samples, and we will make a Federated Identity process with the same Ping Federate server that will play the roles of IdP and SP.

Regarding the main settings of the IdP and SP connections, please refer to the manual. Nevertheless you must pay attention to the base URL you set up and the adapters' name you choose. This base URL is the same than what we entered in the local settings, since the IdP and the SP computers are here the same.

(The full IdP connection and SP connection pages are placed in the appendixes.)

Note that for authentication process, these services do not refer to any databases: the login/passwords to test the applications are stored in a file called [pingfederate-sp-demo.users.props](#) in the SP directory application or [pingfederate-idp-demo.users.props](#) in the IdP directory application.

The main pages of the services you should be able to reach are as follow:

Figure 16: main page of the IdP application sample, case 1

Figure 17: main page of the SdP application sample, case 2

B. Second case: test with ITAM

This case tests both application samples of ITAM and INT, setting a federation of our circles of trust to perform Federated Identity process.

In this case, INT remains an IdP and a SP. Therefore, the test above could still be performed. However, we add in the partners' connections menu of the Ping Federate server ITAM configuration, so that our servers can communicate.

ITAM had chosen to separate the IdP and the SP roles on two servers. **It was really important then to comprehend which ITAM's computer plays either the IdP or the SP role.**

According the configuration ITAM explained

- 'oberon' computer is ITAM's IdP,
- 'titania' computer is ITAM's SP.

To set properly the configuration, you should use the metadata files that your partner gives you. If you do not have them, you need their own Ping Federate server's IdP and SP connections summaries to retrieve their configuration.

Some of the configurations' requirements (such as artefact and redirect bindings) were not given in the Quick Start Guide of Ping Federate. That is why you really have to pay attention of what the partner gives you for information. The following extract shows the parameters, in our case, that we had set up for working with ITAM's configuration:

Adapter Mapping & User Lookup	
Select Adapter Instance	
Selected adapter	SPJava
Adapter Data Store	
Attribute location	Use only the attributes available in the SSO Assertion
Adapter Contract Fulfillment	
userId	SAML_SUBJECT(Assertion)
SSO Service URLs	
Endpoint	URL: /idp/SSO.saml2 (Redirect)
Endpoint	URL: /idp/SSO.saml2 (POST)
SLO Service URLs	
Endpoint	URL: /idp/SLO.saml2 (Redirect)
Endpoint	URL: /idp/SLO.saml2 (POST)
Allowable SAML Bindings	
Artifact	true
POST	true
Redirect	true
Artifact Resolver Locations	
Artifact Resolution Endpoint	index = 0, http://oberon.ipv6.itam.mx:9030/idp/ARS.ssaml2

Figure 18: screenshot of ITAM's IdP connection settings in our server

IdP Adapter Mapping	
Select Adapter Instance	
Selected adapter	IdPJava
Assertion Mapping	
Adapter	PF4 LDAP Authentication Service v1.0
Data Store or Assertion	Use only the Adapter Contract values in the SAML assertion
Attribute Contract Fulfillment	
SAML_SUBJECT	userId(Adapter)
Assertion Consumer Service URL	
Endpoint	URL: http://titania.ipv6.itam.mx:9030/sp/ACS.saml2 (POST)
Endpoint	URL: http://titania.ipv6.itam.mx:9030/sp/ACS.saml2 (Artifact)
SLO Service URLs	
Endpoint	URL: /sp/SLO.saml2 (Redirect)
Endpoint	URL: /sp/SLO.saml2 (POST)
Allowable SAML Bindings	
Artifact	true
POST	true
Redirect	true
Artifact Lifetime	
Artifact Lifetime in seconds	60
Artifact Resolver Locations	
Artifact Resolution Endpoint	index = 0, /sp/ARS.ssaml2

Figure 19: screenshot of ITAM's SP connection settings in our server

Please refer to our Ping Federate server's IdP connection and SP connection pages that are placed in the appendixes for more information when setting the connections parameters.

Since the sample applications are the same for both INT and ITAM, we have made a change in the **pingfederate-idp-demo.users.props**: The username "Joe" and its password have been replaced by the username "Eunice" and password "Eunice".

This can prove that the Federation Identity between INT's and ITAM's circles of trust efficiently works. Indeed, we have been able to connect to the SP application sample of ITAM with a local INT profile ("Eunice" account didn't appear in ITAM accounts' configuration file, but only in our local INT accounts' configuration file).

The SP login page, the IdP an SP main pages of the services you should be able to reach are as follow:

Identity Provider Main Page

This is the main page of the IdP Sample Application.
You can initiate Single Sign on to any of the configured SP connections or perform single logout.

SP Connection ?

Connection Id: titania.ipv6.itam.mx

Click on the image to initiate Single sign on



SP Connection ?

Connection Id: INT-SAML2.0-server

Click on the image to initiate Single sign on



User Attributes ?

authnContext	PASSWORD
userid	idp

Single Logout ?

Click on the link for Single Logout

[Single Logout](#)

Local Logout ?

Click on the link for Local logout

[Local Logout](#)

Figure 20: main page of the IdP application sample (case 2)

Service Provider Login

Local Login ?

Login ID:

Password:

Login through IdP ?

Select an IdP connection from the drop down and click Login.

☐

Figure 21: login page of the SP application sample (case 2)

We can clearly see here that INT's and ITAM's IdP are known from the service.

Figure 22: main page of the application SP application sample (case 2)

C. Third case: test with LDAP

This case tests the PF LDAP adapter, on the IdP side.

It is then possible to test the SP-initiated SSO/SLO, but it works from **both** ITAM and INT's SP application sample.

In that case, the user name is not shown in the login field, as the IdP and SP application samples do, but the user needs to know his (her) login and password.

These can be any of the couple login/password entered in the LDAP database.

Working from the previous case(s), if you need to set up this case, you only have to change 'IdPJava' by 'LDAPINT' – as long as you have created the LDAPINT IdP adapter are we have explained before – in each SP partners' connections you want. The SP login and main pages will remain exactly the same, the only difference will be that you will not be connected to INT's IdP login page as before. A login form will appear, as the one illustrated here:



Figure 23: login popup to initiate SSO

APPENDIXES

<u>POSTFIX MAILSERVER CONFIGURATION FILE</u>	<u>32</u>
<u>VENTENPOUPE COMPUTER .BASHRC FILE</u>	<u>33</u>
<u>CUBITUS COMPUTER .BASHRC FILE</u>	<u>34</u>
<u>IDP CONECTION INT SUMMARY</u>	<u>39</u>
<u>IDP CONECTION ITAM SUMMARY</u>	<u>41</u>
<u>SP CONECTION INT SUMMARY</u>	<u>43</u>
<u>SP CONECTION ITAM SUMMARY</u>	<u>45</u>

Configuration file for the LDAP server

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

#####
# Global Directives:

# Features to permit
allow bind_v2

# Schema and objectClass definitions
include      /etc/ldap/schema/core.schema
include      /etc/ldap/schema/cosine.schema
include      /etc/ldap/schema/nis.schema
include      /etc/ldap/schema/inetorgperson.schema

# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck  on

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile      /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile     /var/run/slapd.args

# Read slapd.conf(5) for possible values
loglevel     0

# Where the dynamically loaded modules are stored
modulepath   /usr/lib/ldap
moduleload   back_bdb

#####
# SSL:
# Uncomment the following lines to enable SSL and use the default
# snakeoil certificates.
#TLSCertificateFile    /etc/ssl/certs/ssl-cert-snakeoil.pem
#TLSCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

#####
# Specific Backend Directives for bdb:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend      bdb
checkpoint 512 30
```

```
#####
# Specific Backend Directives for 'other':
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
#backend          <other>

#####
# Specific Directives for database #1, of type bdb:
# Database specific directives apply to this database until another
# 'database' directive occurs
database          bdb

# The base of your directory in database #1
suffix           "o=INT, c=FR"
rootdn "cn=admin, o=INT, c=FR"
rootpw {SSHA}K2s6Z+Rx4Q/84bE93ji393jxxr5UzPLk

# Where the database file are physically stored for database #1
directory         "/var/lib/ldap"

# Indexing options for database #1
index             objectClass eq

# Save the time that the entry gets modified, for database #1
lastmod           on

# Where to store the replica logs for database #1
# relogfile       /var/lib/ldap/repllog

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
access to attrs=userPassword
    by dn="cn=admin, o=INT, c=FR" write
    by anonymous auth
    by self write
    by * none

# Ensure read access to the base for things like
# supportedSASLMechanisms. Without this you may
# have problems with SASL not knowing what
# mechanisms are available and the like.
# Note that this is covered by the 'access to *'
# ACL below too but if you change that as people
# are wont to do you'll still need this if you
# want SASL (and possible other things) to work
```

```

# happily.
access to dn.base="" by * read

# The admin dn has full write access, everyone else
# can read everything.
access to *
    by dn="cn=admin, o=INT, c=FR" write
    by * read

# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to
#access to dn="*,ou=Roaming,o=morsnet"
#    by dn="cn=admin,dc=nodomain" write
#    by dnattr=owner write

#####
# Specific Directives for database #2, of type 'other' (can be bdb too):
# Database specific directives apply to this database until another
# 'database' directive occurs
#database    <other>

# The base of your directory for database #2
#suffix      "dc=debian,dc=org"

```

Postfix mailserver configuration file

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version

# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${queue_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${queue_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

myhostname = localhost
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = cubitus.int-evry.fr, localhost, localhost.localdomain, localhost
relayhost =
relay_domains =
mynetworks = 127.0.0.0/8
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
notify_classes = resource, software
home_mailbox = Maildir/
```

Ventenpoupe computer .bashrc file

```
# some more ls aliases
#alias ll='ls -l'
#alias la='ls -A'
#alias l='ls -CF'

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
fi

#eunice et pierre
export JAVA_HOME=/home/liberty/JDK/jdk1.5.0_10
export PATH=$JAVA_HOME/bin:$PATH
export PATH=$JAVA_HOME:$PATH

export CLIENT_AXIS=/home/liberty/Client_AXIS

export CLASSPATH=$CLASSPATH:$CLIENT_AXIS/lib/axis-ant.jar
export CLASSPATH=$CLASSPATH:$CLIENT_AXIS/lib/saaj.jar
export CLASSPATH=$CLASSPATH:$CLIENT_AXIS/lib/commons-discovery-0.2.jar
export CLASSPATH=$CLASSPATH:$CLIENT_AXIS/lib/jaxrpc.jar
export CLASSPATH=$CLASSPATH:$CLIENT_AXIS/lib/axis.jar
export CLASSPATH=$CLASSPATH:$CLIENT_AXIS/lib/commons-logging-1.0.4.jar
export CLASSPATH=$CLASSPATH:$CLIENT_AXIS/lib/log4j-1.2.8.jar
export CLASSPATH=$CLASSPATH:$CLIENT_AXIS/lib/wsdl4j-1.5.1.jar
export CLASSPATH=$CLASSPATH:$CLIENT_AXIS/lib/activation.jar
export CLASSPATH=$CLASSPATH:$CLIENT_AXIS/lib/mail.jar
```

Cubitus computer .bashrc file

```
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
[ -z "$PS1" ] && return

# don't put duplicate lines in the history. See bash(1) for more options
export HISTCONTROL=ignoredups

# check the window size after each command and, if necessary,
# update the values of LINES and COLUMNS.
shopt -s checkwinsize

# make less more friendly for non-text input files, see lesspipe(1)
[ -x /usr/bin/lesspipe ] && eval "$(lesspipe)"

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "$debian_chroot" ] && [ -r /etc/debian_chroot ]; then
    debian_chroot=$(cat /etc/debian_chroot)
fi

# set a fancy prompt (non-color, unless we know we "want" color)
case "$TERM" in
xterm-color)

PS1='${debian_chroot:+($debian_chroot)}[\033[01;32m]\u@\h[\033[00m]:[\033[01;34m\
]\w[\033[00m]\$ '
;;
*)
    PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
;;
esac

# Comment in the above and uncomment this below for a color prompt
#PS1='${debian_chroot:+($debian_chroot)}[\033[01;32m]\u@\h[\033[00m]:[\033[01;34m\
\]\w[\033[00m]\$ '

# If this is an xterm set the title to user@host:dir
case "$TERM" in
xterm*|rxvt*)
    PROMPT_COMMAND='echo -ne "\033]0;${USER}@${HOSTNAME}:
${PWD}/${HOME}/~}\007"'
;;
*)
;;
esac
```

```

# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

#if [ -f ~/.bash_aliases ]; then
#   . ~/.bash_aliases
#fi

# enable color support of ls and also add handy aliases
if [ "$TERM" != "dumb" ]; then
    eval "`dircolors -b`"
    alias ls='ls --color=auto'
    #alias dir='ls --color=auto --format=vertical'
    #alias vdir='ls --color=auto --format=long'
fi

# some more ls aliases
#alias ll='ls -l'
#alias la='ls -A'
#alias l='ls -CF'

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
fi

export JAVA_HOME=/home/alliance/jdk1.5.0_10
export PATH=$JAVA_HOME/bin:$PATH

export CATALINA_HOME=/home/alliance/apache-tomcat-5.5.20
export PATH=$CATALINA_HOME/bin:$PATH

export CLASSPATH=$CLASSPATH:$CATALINA_HOME/webapps/axis/WEB-INF/lib/axis-ant.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/webapps/axis/WEB-INF/lib/saaj.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/webapps/axis/WEB-INF/lib/commons-discovery-0.2.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/webapps/axis/WEB-INF/lib/jaxrpc.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/webapps/axis/WEB-INF/lib/axis.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/webapps/axis/WEB-INF/lib/commons-logging-1.0.4.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/webapps/axis/WEB-INF/lib/log4j-1.2.8.jar

```

```

export CLASSPATH=$CLASSPATH:$CATALINA_HOME/webapps/axis/WEB-INF/lib/wsdl4j-1.5.1.jar

export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/activation.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/commons-dbc-1.1.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/jasper-runtime.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/mail.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/servlet.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/servlet-api.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/ant.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/commons-logging-api.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/jdbc2_0-stdext.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/naming-common.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/ant-launcher.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/commons-pool-1.1.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/jndi.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/naming-factory.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/naming-factory-dbc.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/commons-collections.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/jasper-compiler.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/jasper-compiler-jdt.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/jta.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/naming-resources.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/commons-el.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/jsp-api.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/ldap.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/ldapbp.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/providerutil.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/jaas.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/ldapsec.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/commons-discovery-0.2.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/commons-logging-1.0.4.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/common/lib/log4j-1.2.8.jar

#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/tomcat-warp.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/tomcat-jk.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/tomcat-ajp.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/tomcat-apr.jar

```

```

export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/tomcat-jkstatus-
ant.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/tomcat-http11.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/tomcat-http.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/catalina.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/tomcat-coyote.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/commons-modeler.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/commons-
fileupload-1.0.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/servlets-invoker.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/tomcat-jk2.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/servlets-webdav.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/servlets-
cgi.renamet jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/servlets-
ssi.renamet jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/catalina-ant.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/catalina-ant-jmx.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/catalina-cluster.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/catalina-optional.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/catalina-
storeconfig.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/mx4j-jmx.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/jaas.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/commons-
logging.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/tomcat-util.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/servlets-manager.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/servlets-common.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/servlets-default.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/ldapsec.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/jndi.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/ldapbp.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/providerutil.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/ldap.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/jakarta-regexp-
1.3.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/commons-
beanutils.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/lib/commons-
digester.jar
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/webapps/admin/WEB-
INF/lib/struts.jar

export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/webapps/manager/WEB-
INF/lib/commons-fileupload-1.0.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/webapps/manager/WEB-
INF/lib/catalina-manager.jar
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/server/webapps/host-
manager/WEB-INF/lib/catalina-host-manager.jar

```

```
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/webapps/INTest/lib/commons-  
codec-1.3.jar  
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/webapps/INTest/lib/pf4-  
pftoken-agent-1.1.jar
```

```
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/bin/bootstrap.jar  
#export CLASSPATH=$CLASSPATH:$CATALINA_HOME/bin/tomcat-jni.jar  
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/bin/commons-daemon.jar  
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/bin/commons-logging-api.jar  
export CLASSPATH=$CLASSPATH:$CATALINA_HOME/bin/tomcat-juli.jar
```

```
export AXIS_HOME=/home/alliance/axis-1_4  
export PATH=$AXIS_HOME/lib/commons-discovery.jar:$PATH  
export PATH=$AXIS_HOME/lib/commons-logging.jar:$PATH  
export PATH=$AXIS_HOME/lib/jaxrpc.jar:$PATH  
export PATH=$AXIS_HOME/lib/log4j-1.2.4.jar:$PATH  
export PATH=$AXIS_HOME/lib/saaj.jar:$PATH  
export PATH=$AXIS_HOME/lib/wsdl4j.jar:$PATH  
export PATH=$AXIS_HOME/lib/axis.jar:$PATH  
export PATH=$AXIS_HOME/lib/activation.jar:$PATH  
export PATH=$AXIS_HOME/lib/mail.jar:$PATH
```

IdP conection_INT_Summary

 Summary information for your IdP connection. Click on a link to edit a particular configuration setting.

Connection Status ☒ Active
☐ Inactive

Summary

IdP Connection

Role & Protocol

Connection Type	IdP
Protocol	SAML v2.0

General Info

Partner's Entity ID (Connection ID)	INT-SAML2.0-server
Base Url	http://cubitus.int-evry.fr:9030

SAML Profiles

IdP-Initiated SSO	true
IdP-Initiated SLO	true
Attribute Query	false
SP-Initiated SSO	true
SP-Initiated SLO	true

IdP Web SSO

Identity Mapping

Enable Account Mapping	true
------------------------	------

Attribute Contract

Attribute	SAML_SUBJECT
-----------	--------------

Adapter Mapping & User Lookup

Adapter instance name	SPJava
-----------------------	--------

Adapter Mapping & User Lookup

Select Adapter Instance

Selected adapter	SPJava
<u>Adapter Data Store</u>	
Attribute location	Use only the attributes available in the SSO Assertion
<u>Adapter Contract Fulfillment</u>	
userId	SAML_SUBJECT(Assertion)
<u>SSO Service URLs</u>	
Endpoint	URL: /idp/SSO.saml2 (POST)
<u>SLO Service URLs</u>	
Endpoint	URL: /idp/SLO.saml2 (POST)
<u>Allowable SAML Bindings</u>	
Artifact	false
POST	true
Redirect	false
<u>Signature Policy</u>	
Always sign AuthN requests	false
Require digitally signed SAML Assertion	false
<u>Encryption Policy</u>	
Status	Inactive
Credentials	
<u>Digital Signature Settings</u>	
Selected Certificate	CN=Config Signing Cert, O=Sample Organization, C=US
Include Key Info	false
<u>Signature Verification Certificate</u>	
Selected Certificate	CN=Config Signing Cert, O=Sample Organization, C=US
<u>Activation & Summary</u>	
Status	Active

IdP conection_ITAM_Summary

Summary

IdP Connection

Role & Protocol

Connection Type	IdP
Protocol	SAML v2.0

General Info

Partner's Entity ID (Connection ID)	oberon.ipv6.itam.mx
Base Url	http://oberon.ipv6.itam.mx:9030

SAML Profiles

IdP-Initiated SSO	true
IdP-Initiated SLO	true
Attribute Query	false
SP-Initiated SSO	true
SP-Initiated SLO	true

IdP Web SSO

Identity Mapping

Enable Account Mapping	true
------------------------	------

Attribute Contract

Attribute	SAML_SUBJECT
-----------	--------------

Adapter Mapping & User Lookup

Adapter instance name	SPJava
-----------------------	--------

Adapter Mapping & User Lookup

Select Adapter Instance

Credentials

Back-Channel Authentication

Outbound SOAP Authentication Type

SOAP Authentication Type	HTTP Basic
--------------------------	------------

Basic SOAP Authentication (Outbound)

Username	Edith
----------	-------

Digital Signature Settings

Selected Certificate	CN=Config Signing Cert, O=Sample Organization, C=US
----------------------	---

Include Key Info	false
------------------	-------

Signature Verification Certificate

Selected Certificate	CN=Default Config Signing Sert, OU=Dev, O=Ping, L=Denver, ST=CO, C=US
----------------------	---

SP conection_INT_Summary

Summary

SP Connection

Role & Protocol

Connection Type	SP
Protocol	SAML v2.0

General Info

Partner's Entity ID (Connection ID)	INT-SAML2.0-server
Base Url	http://cubitus.int-evry.fr:9030

Assertion Lifetime

Assertion Minutes Before	5
Assertion Minutes After	5

SAML Profiles

IdP-Initiated SSO	true
IdP-Initiated SLO	true
Attribute Query	false
SP-Initiated SSO	true
SP-Initiated SLO	true

SP Web SSO

Identity Mapping

Enable Standard Identifier	true
----------------------------	------

Attribute Contract

Attribute	SAML_SUBJECT
-----------	--------------

IdP Adapter Mapping

Adapter instance name	IdPJava
IdP Adapter Mapping	
<u>Select Adapter Instance</u>	
Selected adapter	IdPJava
<u>Assertion Mapping</u>	
Adapter	PF4 Standard Adapter v1.1
Data Store or Assertion	Use only the Adapter Contract values in the SAML assertion
<u>Attribute Contract Fulfillment</u>	
SAML_SUBJECT	userId(Adapter)
<u>Assertion Consumer Service URL</u>	
Endpoint	URL: /sp/ACS.saml2 (POST)
<u>SLO Service URLs</u>	
Endpoint	URL: /sp/SLO.saml2 (POST)
<u>Allowable SAML Bindings</u>	
Artifact	false
POST	true
Redirect	false
<u>Signature Policy</u>	
Require digitally signed AuthN requests.	false
Always sign the SAML Assertion.	false
<u>Encryption Policy</u>	
Status	Inactive
Credentials	
<u>Digital Signature Settings</u>	
Selected Certificate	CN=Config Signing Cert, O=Sample Organization, C=US
Include Key Info	false
<u>Signature Verification Certificate</u>	
Selected Certificate	CN=Config Signing Cert, O=Sample Organization, C=US
<u>Activation & Summary</u>	
Status	Active

SP conection_ITAM_Summary

Summary

SP Connection

Role & Protocol

Connection Type	SP
Protocol	SAML v2.0

General Info

Partner's Entity ID (Connection ID)	titania.ipv6.itam.mx
Base Url	http://titania.ipv6.itam.mx:9030

Assertion Lifetime

Assertion Minutes Before	5
Assertion Minutes After	5

SAML Profiles

IdP-Initiated SSO	true
IdP-Initiated SLO	true
Attribute Query	false
SP-Initiated SSO	true
SP-Initiated SLO	true

SP Web SSO

Identity Mapping

Enable Standard Identifier	true
----------------------------	------

Attribute Contract

Attribute	SAML_SUBJECT
-----------	--------------

IdP Adapter Mapping

Adapter instance name	LDAPINT
IdP Adapter Mapping	
<u>Select Adapter Instance</u>	
Selected adapter	LDAPINT
<u>Assertion Mapping</u>	
Adapter	PF4 LDAP Authentication Service v1.0
Data Store or Assertion	Use only the Adapter Contract values in the SAML assertion
<u>Attribute Contract Fulfillment</u>	
SAML_SUBJECT	userId(Adapter)
<u>Assertion Consumer Service URL</u>	
Endpoint	URL: http://titania.ipv6.itam.mx:9030/sp/ACS.saml2 (POST)
Endpoint	URL: http://titania.ipv6.itam.mx:9030/sp/ACS.saml2 (Artifact)
<u>SLO Service URLs</u>	
Endpoint	URL: /sp/SLO.saml2 (Redirect)
Endpoint	URL: /sp/SLO.saml2 (POST)
<u>Allowable SAML Bindings</u>	
Artifact	true
POST	true
Redirect	true
<u>Artifact Lifetime</u>	
Artifact Lifetime in seconds	60

Artifact Resolver Locations

Artifact Resolution Endpoint	index = 0, /sp/ARS.ssaml2
------------------------------	---------------------------

Signature Policy

Require digitally signed AuthN requests.	false
--	-------

Always sign the SAML Assertion.	false
---------------------------------	-------

Encryption Policy

Status	Inactive
--------	----------

Credentials

Back-Channel Authentication

Outbound SOAP Authentication Type

SOAP Authentication Type	HTTP Basic
--------------------------	------------

Basic SOAP Authentication (Outbound)

Username	Edith
----------	-------

Back-Channel Authentication

Inbound SOAP Authentication Type

SOAP Authentication Type	HTTP Basic
--------------------------	------------

SSL required	false
--------------	-------

Basic SOAP Authentication (Inbound)

Username	Edith
----------	-------

Digital Signature Settings

Selected Certificate	CN=Config Signing Cert, O=Sample Organization, C=US
----------------------	---

Include Key Info	false
------------------	-------

Signature Verification Certificate

Selected Certificate	CN=Default Config Signing Sert, OU=Dev, O=Ping, L=Denver, ST=CO, C=US
----------------------	---